protiviti®

Face the Future with Confidence

Microsoft Azure Sentinel Implementation Services

Intelligent Security Analytics for the Entire Enterprise

For most organizations, protecting systems, data and users has never been more challenging. Cyber threats are growing rapidly in volume and sophistication, while a cloud-enabled and mobile workforce has restricted visibility and control. Now, more than ever, it is important for organizations to have full visibility across all cloud environments to detect security events and reduce attacker "dwell time."

Microsoft Azure Sentinel, a cloud-native Security Information and Event Management System (SIEM) and SOAR, incorporates the power of AI to deliver intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting and threat response. It eliminates cloud security infrastructure setup and maintenance, while elastically scaling to meet your security needs, reducing IT costs.

Microsoft Azure Sentinel Capabilities

Data Aggregations

- Built on the Azure platform
- Fully integrated with the Azure portal to augment services; e.g., Azure Security Center and Azure Machine Learning
- Connectors providing real-time data integration with Microsoft and 3rd security solutions; leverages Common Event Format, Syslog or REST-API to connect to compliant data sources

Threat Detection

- Out-of-the-box rule templates enable identification and notification of threats
- Templates are centered on known threats, common attack vectors and suspicious-activity escalation chains
- Once enabled, templates can automatically search for suspicious activity

Threat Investigation

- Customizable alerts allow for the aggregation of specific evidence
- Easily investigate the detected threats and incident with an investigation UI
- Readily view the status of each incident and manage the full lifecycle of the event

Threat Response

- Security playbooks in Azure provide built-in templates for manual and automated interdiction
- Playbooks are customizable using Azure Logic Apps
- Proactive response capabilities are enabled via customizable hunting queries

Microsoft Azure Sentinel Implementation Services

Cloud Integration

- Cloud maturity and readiness assessment allows the organization to understand what the Microsoft Azure Sentinel implementation roadmap will require
- Cloud governance, which includes defining and implementing a holistic cloud governance structure to guide and rationalize application services deployed onto the cloud in a risk-sensitive, secure, economical and compliant manner
- Security gap assessment provides identification of analogue processes preventing full digital security visibility
- Integration of legacy systems to enable a hybrid environment

Cybersecurity Intelligence Response Center (CIRC)

- Enhanced “white glove” cybersecurity AAS solution
- Incident triage and containment via Azure Sentinel hunting queries
- Collect and analyze digital evidence
- Ongoing probabilistic cyber risk quantification

Active Security Assessment

- Infrastructure / Application / Network / Database assessment: Leveraging Azure Sentinel to test how a hacker or disgruntled employee could exploit the organization’s IT infrastructure to their advantage
- Executed by probing systems with bespoke simulations designed to allow the organization and the AI engine to refine their understanding of vulnerabilities and deploy mitigating measures
- Monitoring of intelligence sources (i.e., security forums, dark web channels) for new and novel cyber threat methods

Incident Response and Forensics Services

- Pre-incident activities, to include incident response plan (IRP) development and tabletop exercise (TTX) and cyber threat hunting/ breach assessment
- Customization of threat-rule template
- AAS enhanced forensic and incident response capability via rapid alert and automated playbook updates
- Forensic e-discovery support, including forensics evidence collection, support for evidence storage and tracking, evidence hosting and document review

Contact us today to schedule your Microsoft Security Workshop
to get started with Microsoft Azure Sentinel.

Protiviti.com/Microsoft

MicrosoftSolutions@Protiviti.com

TCblog.Protiviti.com

Gold Microsoft Partner

Microsoft

protiviti®

Face the Future with Confidence